Разработка keylogger на python

# Оглавление



## 1.1. Кейлоггер

Кейлоггер – легальная программа (чаще скрытая и используемая злоумышленниками для кражи паролей и другой конфиденциальной информации) по протоколированию нажатий клавиш на клавиатуре или динамике данного процесса. В состав Windows 10/11 входит встроенный кейлоггер, предназначенный для улучшения сервисов письма и наборов текста, как заявляет Microsoft. Коды нажатых клавиш записываются в специальный файл и передаются по определённому адресу. В большинстве случаев шифрование протокола https не предотвращает передачу логированных данных. Регистрация нажатий клавиш может быть выполнена в программном и аппаратном виде. Также существуют методы акустического криптоанализа для распознания нажатий клавиш.

Кейлоггеры могут быть представлены в нескольких основных категориях:

- На уровне ядра. Программа получает root-доступ, скрывая своё присутствие на уровне ядра операционной системы. Такие кейлоггеры наиболее сложны в обнаружении, т.к. зачастую Пользователь даже не имеет root прав. Наиболее часто выполняются в виде драйвера клавиатуры.
- На ровне гипервизора, выступая в роли виртуальной прослойки, работая под операционной системой, не внося в её работу никаких изменений.
- На основе API, перехватывая и опрашивая операционную систему или BIOS на остаточные данные в памяти при вводе ключа.
- На основе таблиц памяти. Подменяют адреса в таблицах, записывая введённые данные в необходимое место.
- По распознаванию рукописного ввода с использованием нейросетей.

Кейлоггер может распространяться в виде части вирусной или троянской программы, так как внедрение его чистом виде является задачей нетривиальной.

Для предотвращения кражи конфиденциальных данных используются различные средства, помогающие при определённых типах кейлоггера: сетевой экран, экранная клавиатура, OTP (одноразовые пароли) и другие.

Задание. Реализовать keylogger на python осуществляющий регистрацию нажатых пользователем клавиш с привязкой ко времени.

### 1.1. Реализация на python

- Для работы с клавиатурой понадобиться подключить модуль **keyboard**

Python keyboard представляет собой библиотеку, которая используется для получения полного контроля над клавиатурой. Она позволяет использовать глобальные события, регистрировать горячие клавиши, имитировать нажатие клавиш клавиатуры для конкретного устройства (с учётом вашей раскладки) и многое другое.

Библиотека позволяет работать под Windows, Unix (необходим **sudo**) и экспериментально на mac os.

- Для работы с другими устройствами ввода, включая клавиатуру может быть использована библиотека **pynput**, позволяющая определять положение курсора, регистрировать щелчки мышью и многое другое
- Для протоколирования времени нажатия клавиш используем Timer из datetime, модуль уже входит в состав python и экспортировать дополнительное его не нужно. Он позволяет управлять датой и временем

  Для получения текущей даты можно использовать следующую конструкцию:

  ```
  from datetime import date
  current_date = date.today()
  print(current_date)
  ```

  Для реализации отслеживания удерживания клавиши потребуется засекать время её нажатия и освобождения:

  *.start_date = datetime.now()

  *.end_date = datetime.now()

Существует специальный объект **Listener**, позволяющий прослушивать события клавиатуры, его необходимо экспортировать следующим образом:

**from pynput import** keyboard

и далее реализовать, например:

listener = keyboard.Listener(on_press=**None**,

on_release=**None**,

suppress=**False**, **kwargs)

Параметры **Listener**:

- **on_press=None** - вызываемый объект, который вызывается при нажатии клавиши. Он будет вызываться с аргументом key, где key - это объекты **keyboard.KeyCode, keyboard.Key** или None, если ключ неизвестен
- on_release=None - вызываемый объект, который вызывается при отпускании клавиши. Он будет вызываться с аргументом **key**, где **key** - смотрите в описании аргумента on_press
- suppress=False - отвечает за подавление событий. Установка этого аргумента в значение True предотвратит передачу событий ввода в остальную часть системы
- **kwargs - параметры управления потоком, а также любые нестандартные платформенно-зависимые опции

- Создаём переменную для хранения log, который будет помещаем в файл log.txt

Необходимо учесть запись специальных клавиш, таких как enter, space … и добавить способ их записи

- Далее необходимо создать метод для записи нажимаемых пользователем клавиш keywrite()
- Поскольку кейлоггер будет запускаться неоднократно необходимо реализовать метод по созданию файла для записи и соответствующего ему названия состоящего из времени запуска программы create_filename()
- Теперь следует записать полученные ранее данные о нажатых клавишах в созданный выше файл с помощью метода report()
  - Пример создания файла test.txt и записью в него текста:

```
with open('test.txt', 'w') as f:
 f.write('Create a new text file!')
```

- Последним шагом создаём метод по запуску самого кейлоггера, который определяет время его включения и осуществляет непосредственный запуск keyloggerstart()
- Как итог следует запустить предоставленную тестовую утилиту KD и с помощью запущенного кейлоггера записать нажатые клавиши. Тестовая утилита выполняет нажатие 5 различных клавиш, привязанных к вашему варианту ЛР.

Параметры итоговой программы:

- Запись времени запуска и остановки программы
- Регистрация набираемых с клавиатуры клавиш, времени их нажатия и освобождения
- Запись лога в файл log.txt в виде:

  Program start at 01.01.2024 00:00:00

  01.01.2024 00:00:00 down ‘key1’

  01.01.2024 00:00:01 release ‘key1’

  …

  Program stop at 01.01.2024 00:00:00